

Illinois Department of Transportation Positive Train Control (IDOT PTC) Project

IDOT PTC Safety Program Overview

W. Klinck

8 November, 2000

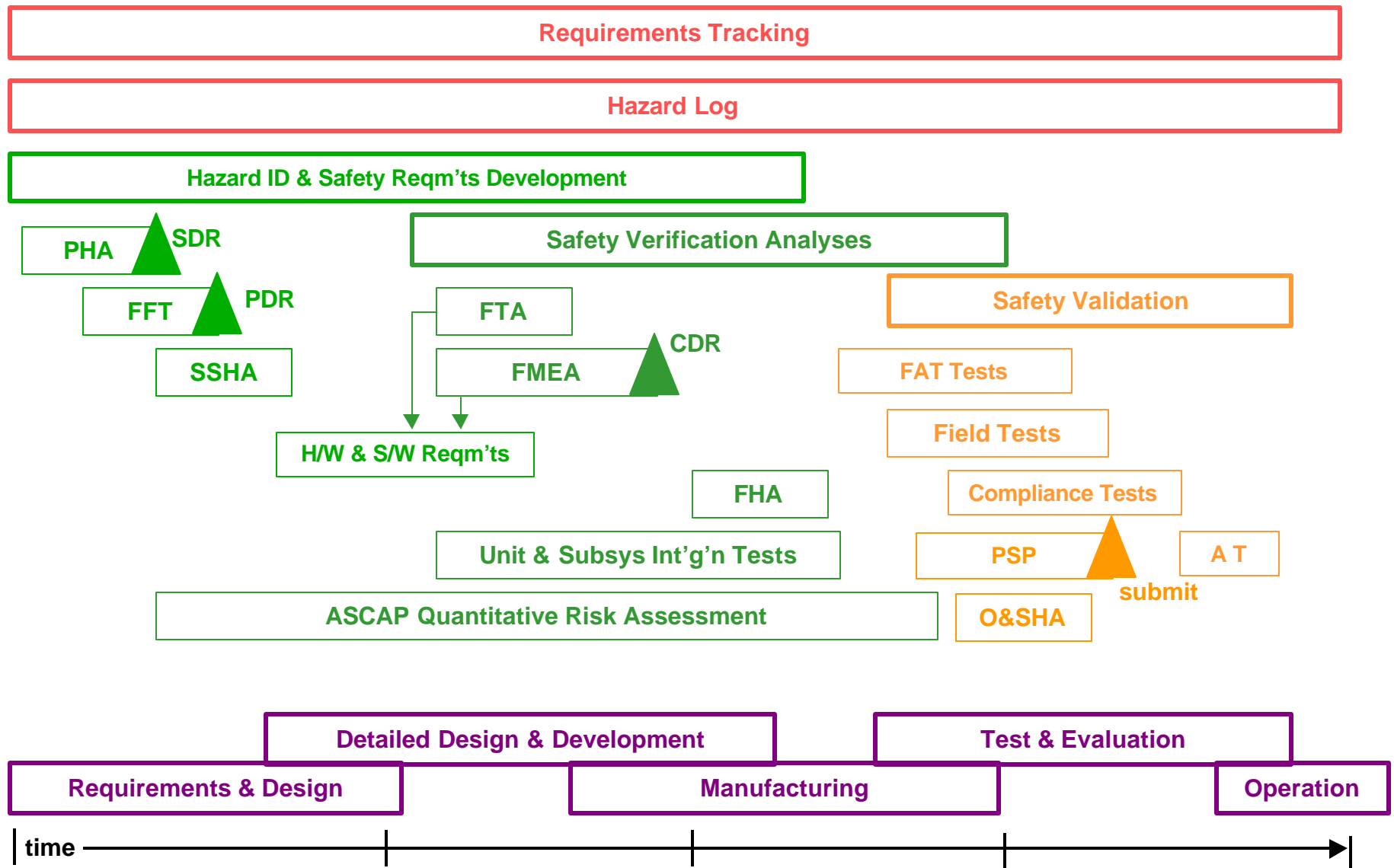
IDOT PTC SAFETY TOPICS

- **SYSTEM REQUIREMENTS & SYSTEM SAFETY ASSURANCE PROCESS**
- **HAZARD AND RISK ANALYSES**
- **SAFETY CRITICAL SYSTEM DEVELOPMENT**
- **FAULT TOLERANCE**
- **SOFTWARE SAFETY**
- **FORMAL METHODS**
- **VERIFICATION, VALIDATION AND TESTING**
- **PRODUCT SAFETY PLAN (PSP)**
- **APPROVAL**

SYSTEM REQUIREMENTS

- **SAFETY REQUIREMENTS SOURCES**
 - **SYSTEM SPEC VERSION 3.0**
 - 20 SAFETY REQUIREMENTS IN PARAGRAPHS 4.11.1 AND 4.11.2
 - **RAILROAD SAFETY PROGRAM PLAN**
 - BASED UPON IEEE P1483 AND MIL-STD-882C
 - **NOTICE OF PROPOSED RULEMAKING**
 - DRAFT #8 UNDER PUBLIC REVIEW
 - **DERIVED REQUIREMENTS FROM SAFETY ANALYSES**

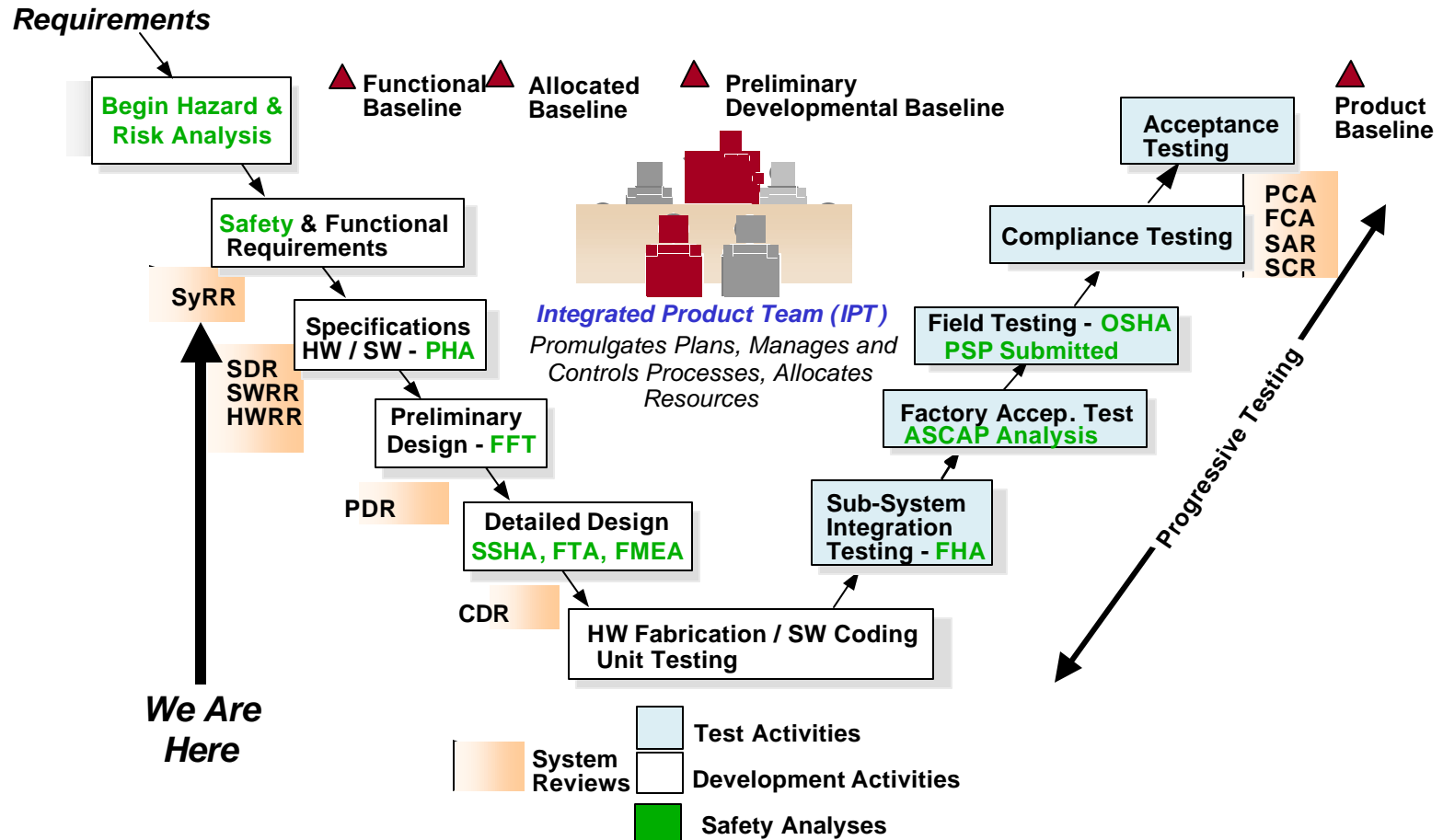
PTC System Safety Assurance Process



HAZARD AND RISK ANALYSES

- **HAZARD ANALYSES - PERFORMED VIA PHA, FFT, SSHA, FTA, FMEA, FHA AND O&SHA**
- **RISK - ADDRESSED VIA AXIOMATIC SAFETY-CRITICAL ASSESSMENT PROCESS (ASCAP) DEVELOPED BY UVA**
 - **MODELS HARDWARE, SOFTWARE, OPERATING RULES, HUMAN INTERACTION**
 - **SIMULATES EVENTS SEQUENCES LEADING TO HAZARD**
 - **MODELS FAILURE PROBABILITIES AND RANDOM FAILURES**
 - **PERFORMS “PROOF OF CORRECTNESS” ANALYSIS**
 - **VERIFY SYSTEM DESIGN (NO FAULTS)**
 - **PERFORMS “PROOF OF SAFETY CRITICAL RISK” ANALYSIS**
 - **INJECTS FAULTS INTO SYSTEM WITH MONTE CARLO (RANDOM NUMBER) STIMULATION OF FAILURES**
 - **VERIFIES FAIL SAFE RESPONSE**
- **OTHER METHODS (E.G. FAULT TREES) MAY ALSO BE APPLIED**

SAFETY CRITICAL SYSTEM DEVELOPMENT



FAULT TOLERANCE

- **HARDWARE TO BE FAULT TOLERANCE - POSSIBLE APPROACHES**

- **FAULT TOLERANCE**

- REDUNDANT PROCESSORS
 - AUTOMATIC FAULT DETECTION
 - HOT REPLACEABLE MODULES
 - GRACEFUL DEGRADATION
 - OPERATING MODES ADAPT TO HARDWARE FAILURES

- **FAULT DETECTION / AVOIDANCE**

- WATCHDOG TIMER
 - DISABLE EXECUTION OF TEST INSTRUCTIONS DURING NORMAL OPERATION
 - DETECT ILLEGAL OPCODES
 - REPEAT SEGMENT-TO-SEGMENT COMMUNICATIONS TO ENSURE ACCURACY AND RECEIPT

- **SOFTWARE FAULT TOLERANCE - ACCOMPLISHED VIA:**

- DATA HIDING / ENCAPSULATION (OBJECT ORIENTATION)
 - RECOVERY BLOCKS TO RE-START PROCESSING AFTER FAULT
 - VOTING / CROSS CHECKING (DETECT FAULTS IN PARALLEL PROCESSORS)
 - AUTOMATICALLY REDISTRIBUTE PROCESSING FUNCTIONS AFTER FAULT
 - I/O DONE USING REQUEST / ACKNOWLEDGE PROCESS
 - REASONABLENESS TESTS TO VERIFY PLAUSIBILITY OF DATA
 - SOFTWARE WATCHDOG TIMERS TO DETECT PROCESSING FAULTS

SOFTWARE SAFETY

- **LANGUAGE SUBSETS UNDER EVALUATION FOR SAFETY**
 - **SUBSETS AVOID AMBIGUOUS FEATURES, FAILURE-PRONE CONSTRUCTS AND PROGRAMMER MISUNDERSTANDING**
 - **SUBSET INFORMATION FROM SEVERAL SOURCES UNDER REVIEW**
- **STATIC CODE ANALYZER TOOLS FILTERS SOURCE CODE PRIOR TO COMPILATION**
 - **STATIC CODE ANALYZER FINDS VIOLATIONS OF LANGUAGE SUBSETS AND OTHER RULES**
 - **OTHER TOOLS IN USE AT LOCKHEED MARTIN WILL ALSO BE EMPLOYED**
 - **IDENTIFY UNINITIALIZED VARIABLES, TYPE MISMATCHES, UNUSED VARIABLES, MEMORY LEAKS, VARIABLES WITH AMBIGUOUS SCOPE**
- **LM USING PROGRESSIVE TESTING METHODS:**
 - **SYSTEM SAFETY DEVELOPMENT PROCESS**
 - **TESTING PERFORMED FROM “BOTTOM UP” TO DETECT AND REMOVE ERRORS AS EARLY AS POSSIBLE IN DEVELOPMENT CYCLE**

FORMAL METHODS

- **DETAILED SPECIFICATIONS FOR HARDWARE, SOFTWARE AND SYSTEM**
 - **SOFTWARE DEVELOPMENT PLAN (SDP)**
 - **SYSTEM SEGMENT DESIGN DOCUMENT (SSDD)**
 - **SOFTWARE REQUIREMENTS SPECIFICATION (SRS)**
 - **HARDWARE REQUIREMENTS SPECIFICATION (HRS)**
 - **INTERFACE DESIGN DOCUMENT (IDD)**
 - **HARDWARE DESIGN DOCUMENT (HDD)**
 - **SOFTWARE DESIGN DOCUMENT (SWDD)**
- **REQUIREMENTS VERIFICATION**
 - **REQUISITE PRO BEING USED TO TRACK, ALLOCATE AND VERIFY / TEST REQUIREMENTS THROUGHOUT THE PROGRAM**

VERIFICATION, VALIDATION AND TESTING

- **VERIFICATION**
 - **CONFIRMS THE DESIGN MEETS THE SPECS**
- **VALIDATION**
 - **VERIFIES THAT THE SPECIFICATION IS ADEQUATE AND CORRECT**
- **TESTING METHOD**
 - **REQUIREMENTS FLOWED DOWN TO TEST PROCEDURES**
 - **PROGRESSIVE TESTING - “BOTTOM UP” METHOD**

IDOT PTC PRODUCT SAFETY PLAN (PSP)



APPROVAL

- **FORMAL PSP IS SUBMITTED TO FRA BY TTCI / UPRR / AMTRAK**
 - **LM GENERATED PSP PROVIDES INPUT AND DETAILED ANALYSES**
 - **PSP SUBMISSION DATE IS JUNE 2002**
- **ACCEPTANCE TESTING CONCLUDES LM's EFFORT**
 - **CONFIRMS FUNCTIONALITY OF ALL 7 BUILDS**
 - **CONFIRMS COMPLIANCE WITH REQUIREMENTS AND STANDARDS**
 - **TRANSFERS OWNERSHIP TO NAJPTC**
 - **1 YEAR WARRANTY BEGINS THEREAFTER**